SECRET

D11

UNITED STATES GOVERNMENT

Memorandum

S-3012/DP-3

TO : DS-6

DATE: 6 February 1973

FROM : DP-3

SUBJECT: Guidance on ADP Multi-Level Security Problems (U)

1. (U) Reference memorandum FOUO-67142/DS-6C3, 2 Feb 1973, subject as above.

2. (C) I appreciate the opportunity to present to you my views on the types of guidance required with reference to the ADP multi-level security problem. In my judgment, this is one of the most complex security issues facing our government today. It will not go away. It will grow in size and complexity in the years to come. It will exert a major influence on intelligence support to Command and Control and to the White House Situation Room. We cannot expect a "once-and-for-all" solution to the multi-level security problem. We can only expect a long series of guidance papers as we progressively increase our understanding of the nature and complexity of this problem.

3. (S) The following, in priority order, are the major areas where I feel that guidance is required with reference to the multi-level security problem:

a. Guidance on the kinds of configurations which can be permitted, given the present state of the art. (For example, should a "programming capability" be permitted at the terminals or only a "query and file update capability.")

b. Designation of the "authority" who is authorized to certify multi-level security ADP systems. DCID 1/16 states that the USIB Members will have this authority. It does not stipulate who has the authority to certify inter-agency computer networks, such as COINS. Also, in DoD, it is not clear whether the Director, DIA must certify all the intelligence ADP systems in the Services and Commands or can delegate this responsibility.

c. Standardization of the physical security regulations for SI and TK material. At present, there is considerable confusion on this issue, especially as it pertains to terminal locations.

d. Guidance on what constitutes "open storage" and "closed storage" with reference to remote terminals.

e. A differentiation between the security regulations pertaining to "inadvertent disclosure" on the one hand, and "malicious penetration" on

DIA review completed.

Classified by DP-3
DIA
SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS
DECLASSIFIED ON 31 DECEMBER 1981

SECRET

the other hand. Our present regulations appear to be overly concerned with "inadvertent disclosure" of material to loyal, in-house people and place very little emphasis on what is required to prevent "malicious penetration" by an enemy agent.

f. An update of the concept of "need-to-know" in order to utilize new technology effectively. At present, the "need-to-know" principle has been virtually abandoned in communications centers, warning centers, NSA, NPIC, etc.

g. Guidance on "foreign disclosure" via computer systems (e.g., on-line access to U.S. ADP systems by foreign nationals).

h. Guidance on the security of automated multi-level displays. This is a growing problem with reference to intelligence support to Command anc Control Centers.

i. Guidance on the multi-level security aspects of closed circuit TV displays. This also is a growing problem with reference to intelligence support to Command and Control Centers.

4. (U) I recognize that the foregoing represents a huge workload for security people. It is important that emphasis be placed in these areas, however. We are entering an era in which there will be less and less hard copy material and more and more "machineable material." Unless our security concepts and regulations keep abreast of this change, the intelligence community will run the risk of extremely serious security breakdowns.

25X1

Assistant Deputy Director for Systems
Deputy Director for Plans